UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Google Pixel 5 smartphone	)	Case No. MJ22-040

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 875(c)	Interstate Threatening Communications

The application is based on these facts:

✓ See Affidavit of FBI Special Agent Joseph Rico, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Joseph Rico, FBI Special Agent

Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or

◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 02/02/2022

Judge's signature

City and state: Seattle, Washington

S. Kate Vaughan, United States Magistrate Judge

Printed name and title

USAO# 2020R00313

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Joseph Rico, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

I am a Special Agent with the Federal Bureau of Investigation (FBI). I am currently assigned to the FBI's Seattle Field Office. I have been employed as a Special Agent since September 2015. Prior to this employment, I was employed as an Intelligence Analyst with the FBI's El Paso Field Office. In total, I have approximately twelve years of federal law enforcement experience.

I am a graduate of the University of Texas at El Paso, where I received a Bachelor of Art in Political Science. I completed a 10-week Intelligence Basic Course and a 23-week Basic Field Training Course at the FBI Academy located in Quantico, Virginia.

I am responsible for domestic terrorism investigations involving specified unlawful activities, to include racially motivated violent crimes that occur in the Western District of Washington. I have actively participated in investigations of criminal activity, including but not limited to crimes against persons, crimes against property, and crimes involving the use of interstate communications. During these investigations, I have also participated in the execution of search warrants and the seizure of evidence indicating the presence of criminal violations. As a law enforcement officer, I have applied for and obtained search and arrest warrants and have executed such warrants.

I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the Google Pixel 5 smartphone that is further described in Attachment A, for the things described in Attachment B. As set forth below, I have probable cause to believe that the Google Pixel 5 smartphone will contain evidence of the offense of Interstate Threatening Communications, in violation of Title 18, United States Code, Section 875(c).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 875(c) will be found on the Google Pixel 5 smartphone.

SUMMARY OF PROBABLE CAUSE

A. AGC Biologics.

AGC Biologics (AGC) is a biotech company headquartered in Bothell, Washington. According to their website, AGC offers "services for the scale-up and cGMP manufacture of protein-based therapeutics, mRNA, pDNA, viral vector and cell therapy products." According to media reports and other open-source information, AGC's Bothell facilities are involved in a partnership to develop and produce components of COVID-19 vaccines.

B. Alleged Bomb Threat on November 19, 2021.

The subject of this investigation is Donovan Steinbarge, who works as a security guard and receptionist at the AGC facilities in Bothell. On November 19, 2021, Steinbarge contacted the AGC Security Manager, Erik White, and claimed that he had received an anonymous phone call during which the caller asked to speak to the AGC CEO and stated, "There's a car bomb in your parking lot." Later that day, Steinbarge showed Security Manager White an email that was sent directly to Steinbarge's AGC email address from ProtonMail account hideandgoseek20212012@protonmail.com. The email had the subject line, "We're hiding," and the body of the email read: "Can you find us???"

In response to the information provided by Steinbarge, AGC shut down its Bothell facilities and reported the threats to the Bothell Police Department. Police officers and bomb technicians responded to the facilities and cleared the area of any threats (no bomb was found).

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

C. Alleged Bomb Threat on December 14, 2021.

On December 14, 2021, Steinbarge reported another bomb threat to Security Manager White. Steinbarge showed White an email he received at his AGC email address sent from ProtonMail address ryanmichaelbey@protonmail.com. The subject line of the email was "Kaboom," and the email read as follows:

> On December 15, 2021, at exactly 3 pm local time, I will park a pick-up truck with a full tank of fuel loaded with 2 20 gallon tanks of diesel fuel next to your liquid oxygen tank. I will then detonate a backpack, also containing steel ball bearing and nails. I will do this unless you IMMEDATELY cease all production of the bioweapon known publicly as the COVID-19 vaccine. You have 24 hours to post evidence of your compliance to agcbio/news. I will be watching.

Upon viewing this email, Security Manager White became suspicious of Steinbarge for three reasons:

First, Steinbarge's AGC email address is not publicly available, and he is not listed as an employee on AGC's public-facing website. Therefore, it would be unlikely for someone to send bomb threats directly to Steinbarge's AGC email address.

Second, the threat contained in the December 14 email – the use of a truck bomb to detonate a liquid oxygen tank – precisely mirrored a recent security briefing that White provided to Steinbarge and other AGC security guards. Specifically, after the November 19 reported threat, White provided the security team with a briefing about potential vulnerabilities at AGC, including the possibility of a vehicle-born explosive device targeting the liquid oxygen tanks.

Third, Steinbarge had previously told White that he uses ProtonMail and extolled the virtues of the ProtonMail service.[1] White noted that both threatening emails were sent to Steinbarge from ProtonMail accounts.

[1] Based on my training and experience, I know that ProtonMail is an end-to-end encrypted email service headquartered in Switzerland. ProtonMail allows for the self-destruction of a user's email and the company has a reputation for being uncooperative with U.S. based law enforcement. These features of ProtonMail can be taken advantage of by individuals

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

On December 14, 2021, White contacted the FBI to report the recent threats and his suspicions that Steinbarge may have been behind them.

C. FBI Interview of Donovan Steinbarge.

On December 15, 2021, I interviewed Steinbarge along with another FBI Special Agent. Steinbarge initially denied that he had ever used ProtonMail. He also denied having received any recent training or security briefings at AGC. We confronted Steinbarge with a posting he made over Twitter in which he stated that he used ProtonMail and commended its security features. At that point, Steinbarge claimed that he previously used ProtonMail but no longer had an account.

Steinbarge consented to agents searching his smartphone, which is the Google Pixel 5 smartphone further described in Attachment A. We began going through the contents of the phone in front of Steinbarge. We opened the Mozilla Firefox browser and accessed ProtonMail. We found the saved log-in information for ProtonMail accounts hideandgoseek@protonmail.com and hideandgoseek20212012@protonmail.com along with saved passwords. As noted above, the alleged November 19 threat was sent to Steinbarge from hideandgoseek20212012@protonmail.com.

We confronted Steinbarge with this information. He then admitted that he was owner and operator of hideandgoseek20212012@protonmail.com. He admitted to sending the November 19 email and said he did so because he wanted to scare his supervisors into taking physical security measures more seriously at AGC. Steinbarge denied sending the December 14 email. At that point, Steinbarge withdrew his consent to search the rest of his smartphone and ended the interview with us.

I am aware that shortly after the interview, AGC fired Steinbarge and he is no longer employed at AGC.

//

//

who wish to hide their identity. Based on open-source information, I am aware that ProtonMail's servers in the United States are located in California, New York, and Illinois.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

INFORMATION ABOUT SMARTPHONES

Cellphones or "Wireless Communication Devices" includes cellular telephones and other devices such as tablets (e.g. iPads and other similar devices) used for voice and data communication through cellular or Wi-Fi signals. These devices send signals through networks of transmitter/receivers, enabling communication with other wireless devices or traditional "land line" telephones. Many such devices can connect to the Internet and interconnect with other devices such as car entertainment systems or headsets via Wi-Fi, Bluetooth or near field communication (NFC). In addition to enabling voice communications, wireless communication devices offer a broad range of capabilities. These capabilities include e-mail and photographs.

Based upon my training and experience, these types of information may be evidence of crimes under investigation. Stored e-mails may contain communications relating to crimes. Photographs on a cellular telephone may help identify the device user, either through his or her own photographs, or through photographs of friends, family, and associates.

Many wireless communication devices including cellular telephones such as the Google Pixel cell phone may also be used to browse and search the Internet. These devices may browse and search the internet using traditional web browsers such as Apple's Safari browser, Google's Chrome browser or Firefox. Based on my training and experience, I know that internet browsing history may include valuable evidence regarding the identity of the user of the device. This evidence may include online usernames, account numbers and e-mail accounts as well as other online services. Internet browsing history may also reveal important evidence about a person's location and search history. Search history is often valuable evidence that may help reveal a suspect's intent and plans to commit a crime or efforts to hide evidence of a crime and may also help reveal the identity of the person using the device.

\\

\\

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Cellphones and other wireless communication devices are also capable of operating a wide variety of communication applications or "Apps" that allow a user to communicate with other devices via a variety of communication channels. These additional communication channels include traditional cellular networks, voice over internet protocol, video conferencing (such as FaceTime and Skype), and a wide variety of messaging applications (such as SnapChat, What'sApp, Signal, Telegram, Viber and iMessage). I know based on my training and experience that there are hundreds of different messaging and conferencing applications available for popular cellular telephones and that the capabilities of these applications vary widely for each application. Some applications include end-to-end encryption that may prevent law enforcement from deciphering the communications without access to the device and the ability to "unlock" the device through discovery of the user's password or other authentication key.

Other communication applications transmit communications unencrypted over centralized servers maintained by the service provider and these communications may be obtained from the service provider using appropriate legal process. Other applications facilitate multiple forms of communication including text, voice, and video conferencing. Information from these communication apps may constitute evidence of the crimes under investigation to the extent they may reveal communications related to the crime or evidence of who the user of the device was communicating with and when those communications occurred. Information from these communication apps may also reveal alias names used by the device owner that may lead to other evidence.

I know based on my training and experience that obtaining a list of all the applications present on a cellphone may provide valuable leads in an investigation. By determining what applications are present on a device, an investigator may conduct follow-up investigation including obtaining subscriber records and logs to determine whether the device owner or operator has used each particular messaging application. This information may be used to support additional search warrants or other legal process to capture those communications and discover valuable evidence.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Cellphones and other wireless communication devices may also contain geolocation information indicating where the device was at particular times. Many of these devices track and store GPS and cell-site location data to provide enhanced location-based services, serve location-targeted advertising, search results, and other content. Numerous applications available for wireless communication devices collect and store location data. For example, when location services are enabled on a handheld mobile device, many photo applications will embed location data with each photograph taken and stored on the device. Mapping applications such as Google Maps may store location data including lists of locations the user has entered into the application. Location information may constitute evidence of the crimes under investigation because that information may reveal whether a suspect was at or near the scene of a crime at any given moment and may also reveal evidence related to the identity of the user of the device.

Based on my training, experience, and research, I know that cellular phones have "Smart Phone" capabilities that allow it to function as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA." In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. In my training and experience, smart phones can act as mini-computers in that they have many of the functionalities of traditional computers.

Searching a cellular phone or wireless communication device is frequently different than conducting a search of a traditional computer. Agents and forensic examiners will attempt to extract the contents of the cellular phone or wireless communication device using a variety of techniques designed to accurately capture the data in a forensically sound manner in order to make the data available to search for the items authorized by the search warrant. This may involve extracting a bit-for-bit copy of the contents of the device or, if such an extraction is not feasible for any particular device, the search may involve other methods of extracting data from the device such as copying the device's active user files (known as a logical acquisition) or copying the device's entire file system (known as a file

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

system acquisition). If none of these methods are supported by the combination of tools available to the examiner and the device to be searched, the agents and examiners may conduct a manual search of the device by scrolling through the contents of the device and photographing the results.

CONCLUSION

Based upon the foregoing information, I believe there is probable cause to search the Google Pixel 5 phone further described in Attachment A for the items described in Attachment B.

Joseph Rico, Affiant
Special Agent, FBI

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit on the 2nd day of February, 2022.

S. KATE VAUGHAN
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A
Property to be Searched

The property to be searched is described as:

A Google Pixel 5 smartphone with IMEI 325493114810048, obtained from Donovan Steinbarge on December 15, 2021, and presently stored in evidence at the Seattle Field Office of the FBI, in Seattle, Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B
Property to be Seized

The smartphone described in Attachment A may be searched for records (in whatever form) that constitute evidence of the crime of Interstate Threatening Communications, 18 U.S.C. § 875(c), including:

a. evidence of who used, owned, or controlled the device;

b. passwords, encryption keys, and other access codes that may be necessary to access the device or to access communication accounts associated with the device;

c. communications made in furtherance of the crime enumerated above;

d. evidence indicating the user's state of mind as it relates to the crime enumerated above;

e. evidence indicating how and when the subject device was accessed or used, to determine the geographic and chronological context of device access and use, in relation to the crime under investigation and to the device user;

f. photographic or video images related to the crime enumerated above.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970